UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/806,435	03/30/2001	Steffen Fries	1454.1053/MJ	1344

21171 7590 11/24/2004

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
HUA, LY	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 11/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/806,435	FRIES ET AL.	
	Examiner	Art Unit	
	Ly V. Hua	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 March 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *13-63* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *49* is/are allowed.

6)☒ Claim(s) *13,14,22,23,27,28,36,37,43, 44, 45-48,50,51 and 57-62* is/are rejected.

7)☒ Claim(s) *15-21,24-26,29-35,38-42,52-56 and 63* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *5/23/2001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Two of the references cited in FORM PTO-1449 have not been considered because the Applicant has not made them available to the examiner. Hard copy of each of those references is hereby requested.

2. Even though the drawings are available in the application, but it appears that they are part of the PCT/DE99/02844 application, rather than of the present application. Attached at the end of this Detailed Action is an Eden print out showing that the drawings are not available as content in the present application. The applicant is to formally file the drawings for the present application.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> . The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 43, 57, 45, 59, 46-48 and 60-62 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

5. With regard to claims 43 and 57:
   a. The phrase "the password" in the ascertaining step (second occurrence) lacks proper antecedent basis.
      i Notice that it is not clear whether the phrase refers to the password ascertained from the authentication toke or the stored password or the password comprised in the password message.
      ii Perhaps the phrase should be changed to –the password message--.
   b. The word "ascertaining" in its context as in the phrase "ascertaining the updated password using the password" appears to be confusing in that it is not clear what is being done to (or how the password is used) to ascertain the updated password.
   c. The purpose for which the step of ascertaining the updated password using the password is performed is not clear since the result of the ascertaining is not being used.
6. With regard to claims 44 and 58:
   a. These claim depend on claims 43 and 48 respectively, and thus each inherits the problem of indefiniteness from its parent claim.
7. With regard to claims 45 and 59:
   a. The phrase "the password" in the ascertaining step (second occurrence) lacks proper antecedent basis.
      i Notice that it is not clear whether the phrase refers to the password ascertained from the authentication toke or the stored password or the password comprised in the password message.
      ii Perhaps the phrase should be changed to –the password message--.
   b. The word "ascertaining" in its context as in the phrase "ascertaining the updated password using the password" appears to be confusing in that it is not clear what is being done to (or how the password is used) to ascertain the updated password.
   c. The purpose for which the step of ascertaining the updated password using the password is performed is not clear since the result of the ascertaining is not being used.
8. With regard to claims 46-48:
   a. These claims depend on claim 45 and thus inherit the problem of indefiniteness therefrom.
9. With regard to claims 60-62:
   a. These claims depend on claim 50 and thus inherit the problem of indefiniteness therefrom.

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

.(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

Note: The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

11. Claims 13, 14, 27, 28, 36,37, 50, 51, 22, 23 are rejected under 35 U.S.C. 102(e) as being anticipated by Barry et al (6,615,258 hereinafter Barry).

12. As to claims 13 and 14:
- a. Barry et al (6,615,258 hereinafter Barry) teaches [Fig. 7; col. 18, line 56 to col. 19, line 16] a method
  - i for updating a password
  - ii between
    - (1) a first computer [154] and
    - (2) a second computer [39],
  - iii comprising:
    - (1) receiving
      - (a) at the second computer
      - (b) a service request message
        - (i) transmitted by the first computer
          - 1) over a communication link [Internet Infrastructure] existing between the first computer and the second computer,
        - (ii) the service request message
          - 1) containing the password, and
          - 2) being used to request provision of a service;
    - (2) checking [i.e., looking for a match of the password],
      - (a) at the second computer,
      - (b) whether the password
        - (i) contained in the service request message
        - (ii) is valid [e.g., expired] for the first computer;
    - (3) providing,
      - (a) if the password is valid [i.e., if a match is found in a security profile],
      - (b) the service;
    - (4) transmitting,
      - (a) if the password is invalid [e.g., if the password is expired],
      - (b) from the second computer
      - (c) to the first computer
      - (d) an update message [e.g., "change password request"]
        - (i) to request that the password be updated; and
    - (5) forming [i.e., updating]
      - (a) an updated password.

13. As to claims 27 and 28:
- a. Claims 27 and 28 have limitations that are similar to those of claim 13 and 14 and thus are rejected with the same

reasons applied against claims 13 and 14.

b. It is inherent that the method of Barry's second computer [39] is caused to run by a program stored in a computer readable medium. This is because Barry's element 39 is a computer.

14. As to claims 36 and 37:

a. Claim 36 and 37 have limitations that are similar to those of claim 13 and 14 and thus are rejected with the same reasons applied against claims 13 and 14.

b. Claim 13 has been address above as Barry teaches [Fig. 7; col. 18, line 56 to col. 19, line 16] a method
   i for updating a password
   ii between
      (1) a first computer [154] and
      (2) a second computer [39],
   iii comprising:
      (1) receiving
         (a) at the second computer
         (b) a service request message
            (i) transmitted by the first computer
               1) over a communication link [Internet Infrastructure] existing between the first computer and the second computer,
            (ii) the service request message
               1) containing the password, and
               2) being used to request provision of a service;
      (2) checking [i.e., looking for a match of the password],
         (a) at the second computer,
         (b) whether the password
            (i) contained in the service request message
            (ii) is valid [e.g., expired] for the first computer;
      (3) providing,
         (a) if the password is valid [i.e., if a match is found in a security profile],
         (b) the service;
      (4) transmitting,
         (a) if the password is invalid [e.g., if the password is expired],
         (b) from the second computer
         (c) to the first computer
         (d) an update message [e.g., "change password request"]
            (i) to request that the password be updated; and
      (5) forming [i.e., updating]
         (a) an updated password.

c. The reason for rejecting claim 13 is also applied against claim 36.

15. As to claims 50 and 51:

a. Claim 50 has limitations that are similar to those of claims 13 and 36 and thus is rejected with the same reasons applied against claims 13 and 36.

b. Claim 36 has been addressed above as Claim 36 has limitations that are similar to those of claim 13 and thus is rejected with the same reasons applied against claim 13, which Claim 13 has been addressed above as Barry teaches [Fig. 7; col. 18, line 56 to col. 19, line 16] a method
   i for updating a password
   ii between
      (1) a first computer [154] and
      (2) a second computer [39],
   iii comprising:
      (1) receiving
         (a) at the second computer
         (b) a service request message
            (i) transmitted by the first computer
               1) over a communication link [Internet Infrastructure] existing between the first computer and

the second computer,
(ii) the service request message
1) containing the password, and
2) being used to request provision of a service;
(2) checking [i.e., looking for a match of the password],
(a) at the second computer,
(b) whether the password
(i) contained in the service request message
(ii) is valid [e.g., expired] for the first computer;
(3) providing,
(a) if the password is valid [i.e., if a match is found in a security profile],
(b) the service;
(4) transmitting,
(a) if the password is invalid [e.g., if the password is expired],
(b) from the second computer
(c) to the first computer
(d) an update message [e.g., "change password request"]
(i) to request that the password be updated; and
(5) forming [i.e., updating]
(a) an updated password.

c. The reason for rejecting claim 13 is also applied against claim 36 and claim 50.

16. As to claims 22 and 23:

a. Claims 22 and 23 have limitations that are similar to those of claims 13 and 14 and thus are rejected with the same reason applied against claims 13 and 14 above.

b. Claim 13 has been addressed above as Barry teaches [Fig. 7; col. 18, line 56 to col. 19, line 16] a method
i for updating a password
ii between
(1) a first computer [154] and
(2) a second computer [39],
iii comprising:
(1) receiving
(a) at the second computer
(b) a service request message
(i) transmitted by the first computer
1) over a communication link [Internet Infrastructure] existing between the first computer and the second computer,
(ii) the service request message
1) containing the password, and
2) being used to request provision of a service;
(2) checking [i.e., looking for a match of the password],
(a) at the second computer,
(b) whether the password
(i) contained in the service request message
(ii) is valid [e.g., expired] for the first computer;
(3) providing,
(a) if the password is valid [i.e., if a match is found in a security profile],
(b) the service;
(4) transmitting,
(a) if the password is invalid [e.g., if the password is expired],
(b) from the second computer
(c) to the first computer
(d) an update message [e.g., "change password request"]
(i) to request that the password be updated; and
(5) forming [i.e., updating]
(a) an updated password.

c. With regard to the element of the system as claimed in claim 22, Barry shows [Fig. 7; col. 18, line 56 to col. 19,

line 16, lines 17-67] a system
i for updating a password
ii between first and second computers [154 and 39],
iii comprising:
(1) a receiving unit [inherent in element 39] to receive
(a) at a second computer [39]
(b) a service request message
(i) transmitted
1) by the first computer [154]
2) over a communication link [Internet Infrastructure] existing between the first computer and the second computer,
(ii) the service request message
1) containing the password, and
2) being used to request provision of a service;
(2) a checking unit [inherent in element 39] to check [by searching and matching the password received against the password stored in a security profile in database 160]
(a) at the second computer,
(b) whether the password
(i) contained in the service request message
(ii) is valid for the first computer;
(3) a providing unit [inherent in element 39] to provide,
(a) if the password is valid,
(b) the service requested [e.g., retrieving and providing at the request of a user, who uses element 154, an application entitlement list (col. 19, lines 17-53)];
(4) a transmission unit [inherent in element 39] to transmit,
(a) if the password is invalid [e.g., expired],
(b) from the second computer
(c) to the first computer,
(d) an update message [e.g., "change password request"],
(i) the update message being used to request that the password be updated; and
(5) a forming unit [inherent in element 39] to form [i.e., to updates the password for a given user in its user profile stored in database 160]
(a) an updated password.

Claim Rejections - 35 USC § 103

17. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

.(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

18. Claims 43 and 57 are rejected under 35 U.S.C. 103(a) as being obvious over Barry et al (6,615,258 hereinafter Barry) in view of Hardy et al (6,073,242 hereinafter Hardy) and Swift et al. (5,719,941 hereinafter Swift).

19. As to claim 43,
    a. Barry teaches [col. 18, lines 30-55; col. 18, line 56 to col. 19, line 16; col. 20, lines 38-39] a method which is:
        i for updating a password, and
        ii comprising:
            (1) receiving
                (a) a service request
                    (i) requesting a service,
                    (ii) comprising a password, (rather than an authentication token from which a password can be "ascertained");
            (2) ascertaining (inherently since the validation of the password requires the password for looking up for a match with one the has been stored in profile database 160)
                (a) a password
                (b) (but not from an authentication token);
            (3) determining (by looking up for a match)
                (a) whether the password matches a stored password;
            (4) determining
                (a) validity of the password
                (b) if the password matches a stored password;
            (5) providing [col. 19, lines 1-6]
                (a) the service
                (b) if the password is valid [not expired but found in the profile database 160];
            (6) transmitting,
                (a) an update message requesting that the password be updated
                (b) if the password is invalid [e.g., expired];
            (7) receiving
                (a) a password message
                    (i) comprising an updated password;
            (8) (inherently) checking the integrity (e.g. reliability, error free) of the password message, {which checking is inherently in the server 39 of Barry because without such integrity/error checking, the password message would be erroneous due to noise interference in the transmission propagating from the first computer to the second computer – error checking of message integrity is a must in reliable network system, other wise the system such as that of Barry would render erroneous and not reliable}.
            (9) storing the updated password -- [col. 18, lines 30-36 "server 39 ... storing all security information such as passwords ... which may be requested by ... clients in the network"]; and
            (10) providing the service – [col. 20, lines38-39].
    b. However, Barry
        i does not explicitly teach:
            (1) that his service request message comprises an authentication token, from which a password is to be ascertained; and
            (2) the step of ascertaining/determining
                (a) an update password
                (b) using the password,

ii because Barry appears to have no concern about protecting both passwords (the password in the service request and the updated password in the password message) since they could be intercept and misused by eave droppers; and

c. With regard to the authentication, Hardy et al (6,073,242 hereinafter Hardy) teaches [col. 14, lines 48-50]:
   i token for used in authentication could be a password, an object (a Java object, KeyKOS keys, etc.) or any other king of toke that is trusted.

d. With regard to the ascertaining/determining an update password using the password (or rather using the password massage), Swift et al. (5,719,941 hereinafter Swift) teaches [claims 1, 10, 16 and 18]
   i new password is encrypted for transmission,
   ii decrypting encrypted password once received to ascertain/determine/obtain the new password for authentication purpose.

e. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:
   i use the teaching of Hardy to secure the transmission of Barry's password; and
   ii use the teaching of Swift to secure the transmission of Barry's new password.

f. The skilled person would have been motivated to use the teaching of Hardy and Swift as such because:
   i they secure the password being sent in a network.

20. As to claim 57:
   a. This claim has limitations that are similar to those of claim 43 and thus is rejected with the same reason applied against claim 43 above.

Objections to Claims

21. Claims 15-21, 24-26, 29-35, 38-42 and 52-56 are objected to as they depend on claims that are rejected.

22. Claim 63 is objected to as it has the following minor informality:
   a. The phrase "a ... medium controlling a first computer a second computer and comprising a process of ..." appears to be confusing.
      i Notice that it appears that a word is missing between "a first computer" and "a second computer", which word is to indicate that the controlling is action on the first computer and the second computer.
      ii The applicant is suggested to insert the "and" conjunction between the phrases "a first computer" and "a second computer".

Allowance of Claims

23. Claim 49 is allowed.

Statement of reasons for allowance

24. The Examiner hereby provides reasons for indicating allowable subject matter in each of the claims 49 and 63. Each of Applicant's claim invention presented in claim 49 and claim 63 is directed to various combinations of features. The patentability of this claim resides in every feature of the recited combination of features of the claim. The prior art of record fail to teach or suggest the combination of such features in the sequence of occurrence as shown in the following table.

25. 49. A method a. for updating a password b. between a first computer and a second computer, c. comprising: i entering (1) via the first computer (2) a criteria for a database query; ii receiving (1) at the second computer (2) a service request message	26. 63. A computer readable storage medium a. controlling a first computer ------ a second computer and b. comprising a process of i entering (1) via the first computer (2) a criteria for a database query; ii receiving (1) at the second computer (2) a service request message (a) based on the database query,

(a) based on the database query,
(b) the service request message
(i) requesting a service and
(ii) comprising an authentication token to authenticate the first computer;

iii authenticating
(1) the first computer
(2) using the authentication token in the service request message;

iv ascertaining
(1) a password from the authentication token from the first computer;

v determining
(1) whether the password from the first computer
(a) matches a stored password in the second computer;

vi determining
(1) validity of the password at the second computer
(2) at the second computer
(3) if the password matches the stored password,
(4) wherein the determining the validity of the password comprises
(a) ascertaining
(i) a current time at which the service request message is received,
(b) determining
(i) a first time statement indicating a time at which the password is formed, and
(c) determining
(i) a second time statement indicating a period of time for which the password is valid,
(5) wherein the password
(a) is valid
(b) if the current time is less or equal to a summation of the first time statement and the second time statement;

vii providing
(1) the service request to the first computer
(2) if the password is valid;

viii transmitting
(1) to the first computer
(2) an updated message requesting that the password be updated
(3) if the password is invalid;

ix receiving
(1) at the second computer
(2) a password message
(a) transmitted by the first computer,
(b) wherein the password message comprises
(i) an integrity statement
1) to check the integrity of the password message from the first computer;

x checking the integrity of the password message;

xi ascertaining the updated password; and

xii storing in the second computer the updated password and

xiii providing the service to the first computer.

(b) the service request message
(i) requesting a service and
(ii) comprising an authentication token to authenticate the first computer;

iii authenticating
(1) the first computer
(2) using the authentication token in the service request message;

iv ascertaining
(1) a password from the authentication token from the first computer;

v determining
(1) whether the password from the first computer
(a) matches a stored password in the second computer;

vi determining
(1) validity of the password at the second computer
(2) at the second computer
(3) if the password matches the stored password,
(4) wherein the determining the validity of the password comprises
(a) ascertaining
(i) a current time at which the service request message is received,
(b) determining
(i) a first time statement indicating a time at which the password is formed, and
(c) determining
(i) a second time statement indicating a period of time for which the password is valid,
(5) wherein the password
(a) is valid
(b) if the current time is less or equal to a summation of the first time statement and the second time statement;

vii providing
(1) the service request to the first computer
(2) if the password is valid;

viii transmitting
(1) to the first computer
(2) an updated message requesting that the password be updated
(3) if the password is invalid;

ix receiving
(1) at the second computer
(2) a password message
(a) transmitted by the first computer,
(b) wherein the password message comprises
(i) an integrity statement
1) to check the integrity of the password message from the first computer;

x checking the integrity of the password message;

xi ascertaining the updated password; and

xii storing in the second computer the updated password and

xiii providing the service to the first computer.

27. The Examiner hereby provides reasons for indicating allowable subject matter in claims 45 and likewise claim 59. Each of Applicant's claim invention presented in claim 45 and claim 59 is directed to various combinations of features. The patentability of this claim resides in every feature of the recited combination of features of the claim. The prior art of record fail to teach or suggest the combination of such features in the sequence of occurrence as shown in the following table.

28. 45. A method a. for updating a password of a computer, b. comprising: i receiving (1) a service request message (a) requesting a service and (b) comprising an authentication token; ii authenticating (1) the computer (2) using the authentication token in the service request message; iii ascertaining (1) a password (2) from the authentication token; iv determining (1) whether the password matches a stored password; v determining (1) if the password matches a stored password (2) validity of the password; vi providing, (1) if the password is valid, (2) the service; vii transmitting, (1) if the password is invalid, (2) to the computer (3) an update message requesting that the password be updated; viii receiving (1) a password message (a) from the computer (b) comprising an updated password, (i) where the updated password can be ascertained only by using the password; ix checking the integrity of the password message; x ascertaining (1) the updated password (2) using the password; and xi storing the updated password and xii providing the service.	29. 59. A computer readable storage medium a. controlling a computer and b. comprising a process of: i receiving (1) a service request message (a) requesting a service and (b) comprising an authentication token; ii authenticating (1) the computer (2) using the authentication token in the service request message; iii ascertaining (1) a password (2) from the authentication token; iv determining (1) whether the password matches a stored password; v determining (1) validity of the password (2) if the password matches a stored password; vi providing, (1) if the password is valid, (2) the service; vii transmitting, (1) if the password is invalid, (2) to the computer (3) an update message requesting that the password be updated; viii receiving (1) a password message (a) from the computer (b) comprising an updated password, (i) where the updated password can be ascertained only by using the password; ix checking the integrity of the password message; x ascertaining (1) the updated password (2) using the password; and xi storing the updated password and xii providing the service.

30. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

31. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ly V. Hua whose telephone number is 571-272-3853. The examiner can normally be reached on Monday to Friday from 9:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Vu Kim, can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov.

32. The applicant is hereby notified that:
    a. The new phone number for TC 2100 receptionist is (571) 272-2100.

Ly V. Hua
Primary Examiner
Art Unit 2135

Lvh
November 18, 2004